m.lt

PCT/EP 99/06580

BUNDESREPUBLIK DEUTSCHLAND

EP 99/6580

EJW

Bescheinigung

09/763621

Die Giesecke & Devrient GmbH in München/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Zugriffsgeschützter Datenträger"

am 11. September 1998 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig die Symbole G 06 K und H 04 L der Internationalen Patentklassifikation erhalten.

München, den 30. September 1999

Deutsches Patent- und Markenamt

Der Präsident

Im Auftrag

Hiebinger

Aktenzeichen: 198 41 676.8

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

A 9161
06.90
11/98

Zugriffsgeschützter Datenträger

Die Erfindung betrifft einen Datenträger, der einen Halbleiterchip aufweist, in dem geheime Daten abgespeichert sind. Insbesondere betrifft die Erfindung eine Chipkarte.

Datenträger die einen Chip enthalten, werden in einer Vielzahl von unterschiedlichen Anwendungen eingesetzt, beispielsweise zum Durchführen von Finanztransaktionen, zum Bezahlen von Waren oder Dienstleistungen, oder als Identifikationsmittel zur Steuerung von Zugangs- oder Zutrittskontrollen. Bei allen diesen Anwendungen werden innerhalb des Chips des Datenträgers in der Regel geheime Daten verarbeitet, die vor dem Zugriff durch unberechtigte Dritte geschützt werden müssen. Dieser Schutz wird unter anderem dadurch gewährleistet, daß die inneren Strukturen des Chips sehr kleine Abmessungen aufweisen und daher ein Zugriff auf diese Strukturen mit dem Ziel, Daten, die in diesen Strukturen verarbeitet werden, auszuspähen, sehr schwierig ist. Um einen Zugriff weiter zu erschweren, kann der Chip in eine sehr fest haftende Masse eingebettet werden, bei deren gewaltsamer Entfernung das Halbleiterplättchen zerstört wird oder zumindest die darin gespeicherten geheimen Daten vernichtet werden. Ebenso ist es auch möglich, das Halbleiterplättchen bereits bei dessen Herstellung mit einer Schutzschicht zu versehen, die nicht ohne Zerstörung des Halbleiterplättchens entfernt werden kann.

Mit einer entsprechenden technischen Ausrüstung, die zwar extrem teuer aber dennoch prinzipiell verfügbar ist, könnte es einem Angreifer möglicherweise gelingen, die innere Struktur des Chips freizulegen und zu untersuchen. Das Freilegen könnte beispielsweise durch spezielle Ätzverfahren oder durch einen geeigneten Abschleifprozeß erfolgen. Die so freigelegten

Strukturen des Chips, wie beispielsweise Leiterbahnen, könnten mit Mikrosonden kontaktiert oder mit anderen Verfahren untersucht werden, um die Signalverläufe in diesen Strukturen zu ermitteln. Anschließend könnte versucht werden, aus den detektierten Signalen geheime Daten des Datenträgers, wie z.B. geheime Schlüssel zu ermitteln, um diese für Manipulationszwecke einzusetzen. Ebenso könnte versucht werden, über die Mikrosonden die Signalverläufe in den freigelegten Strukturen gezielt zu beeinflussen.

Der Erfindung liegt die Aufgabe zugrunde, geheime Daten, die in dem Chip eines Datenträgers vorhanden sind, vor unberechtigtem Zugriff zu schützen.

Diese Aufgabe wird durch die Merkmalskombinationen der Ansprüche 1 und 9 gelöst.

Die erfindungsgemäße Lösung zielt im Gegensatz zum Stand der Technik nicht darauf ab, ein Freilegen der internen Strukturen des Chips und ein Anbringen von Mikrosonden zu verhindern. Es werden stattdessen Maßnahmen getroffen, die es einem potientellen Angreifer erschweren, aus den gegebenenfalls abgehörten Signalverläufen Rückschlüsse auf geheime Informationen zu schließen. Diese Maßnahmen bestehen erfindungsgemäß darin, sicherheitsrelevante Operationen so zu manipulieren, daß die bei der Durchführung dieser sicherheitsrelevanten Operationen verwendeten Geheimdaten nicht ohne Hinzunahme weiterer geheimer Informationen ermittelbar sind. Hierzu werden die sicherheitsrelevanten Operationen vor ihrer Ausführung mit Hilfe geeigneter Funktionen verfremdet oder verfälscht. Um insbesondere eine statistische Auswertung bei mehrfacher Ausführung der sicherheitsrelevanten Operationen zu erschweren oder gar unmöglich zu machen, fließt in die Verfremdungsfunktion eine Zufallkomponente ein.

Dies hat zur Folge, daß ein Angreifer aus gegebenenfalls abgehörten Datenströmen die Geheimdaten nicht ermitteln kann.

Die sicherheitsrelevante Operation wird im folgenden von der Funktion h repräsentiert, die Eingangsdaten x auf Ausgangsdaten y abbildet, d.h. $y = h(x)$. Um ein Ausspähen der geheimen Eingangsdaten x zu verhindern, wird gemäß der Erfindung eine verfremdete Funktion h_{R1R2} ermittelt, so daß gilt

$$y \otimes R_2 = h_{R1R2}(x \otimes R_1).$$

Die sicherheitsrelevante Operation wird nunmehr mittels der verfremdeten Funktion h_{R1R2} durchgeführt, deren Eingangsdaten nicht die echten Geheimdaten x sind, sondern verfremdete Geheimdaten $x \otimes R_1$, die durch Verknüpfen der echten Geheimdaten x mit einer Zufallszahl R_1 erzeugt wurden. Ohne Kenntnis der Zufallszahl R_1 können die echten Geheimdaten x aus den verfremdeten Geheimdaten $x \otimes R_1$ nicht ermittelt werden. Als Ergebnis der Anwendung der verfremdeten Funktion h_{R1R2} auf die verfremdeten Geheimdaten $x \otimes R_1$ erhält man verfremdete Ausgangsdaten $y \otimes R_2$. Aus den verfremdeten Ausgangsdaten $y \otimes R_2$ lassen sich durch eine geeignete Verknüpfung die Ausgangsdaten y ermitteln. Vor jeder erneuten Durchführung der sicherheitsrelevanten Funktion können neue Zufallszahlen R_1 und R_2 vorgegeben werden, aus denen jeweils eine neue verfremdete Funktion h_{R1R2} ermittelt wird. Alternativ dazu können mehrere verfremdete Funktionen h_{R1R2} fest abgespeichert sein, von denen vor Durchführung der sicherheitsrelevanten Operation jeweils eine zufällig ausgewählt wird. Dabei ist es besonders vorteilhaft zwei Funktionen h_{R1R2} und $h_{R1'R2'}$ zu verwenden, bei denen die Zufallszahlen R'_1 und R'_2 die bzgl der für die Verfremdung gewählten Verknüpfungsart inversen Werte der Zufallszahlen R_1 und R_2 sind. In einer weiteren Variante können die Zufallszahlen R_1 und R_2 auch gleich sein.

Insbesondere können die Zufallszahlen R_1 und R_2 statistisch unabhängig gewählt werden, so daß es keine Korrelation zwischen Ein- und Ausgangsdaten gibt, die für einen Angriff verwendet werden können.

Werden vor oder nach der hier betrachteten sicherheitsrelevanten Operation h noch weitere Operationen abgearbeitet, so können die Zufallszahlen R_1 und R_2 auch zur Verfremdung der mit den weiteren Operationen bearbeiteten Daten benützt werden.

Besonders vorteilhaft läßt sich die erfindungsgemäße Lösung bei sicherheitsrelevanten Operationen einsetzen, die nichtlineare Funktionen beinhalten. Bei nichtlinearen Funktionen können bereits bekannte Schutzmaßnahmen, die auf einer Verfremdung der Geheimdaten vor der Ausführung der Funktionen basieren, nicht angewendet werden. Die bekannten Schutzmaßnahmen setzten nämlich voraus, daß die Funktionen linear bezüglich der Verfremdungsoperationen sind, damit die Verfremdung nach Ausführung der Funktionen wieder rückgängig gemacht werden kann. Bei der erfindungsgemäßen Lösung werden aber nicht nur die Geheimdaten verfälscht oder verfremdet, sondern auch die sicherheitsrelevanten Operationen, die die Geheimdaten verarbeiten. Die Verfremdung der Geheimdaten und der sicherheitsrelevanten Operationen werden dabei so aufeinander abgestimmt, daß aus den verfremdeten Geheimdaten nach Durchführung der sicherheitsrelevanten Operationen die echten Geheimdaten abgeleitet werden können. Die Abstimmung zwischen der Verfremdung der Geheimdaten und der sicherheitsrelevanten Operationen läßt sich besonders einfach realisieren, wenn die sicherheitsrelevanten Operationen in Form von Tabellen, sogenannten Look-up-tables, realisiert sind. In den genannten Tabellen ist jedem Eingangswert x ein Ausgangswert y zugeordnet. Die Ausführung der durch die

Tabellen realisierten Funktionen erfolgt durch Nachschlagen der zu den jeweiligen Eingangswerten x gehörigen Ausgangswerte y.

Die Erfindung wird nachstehend anhand der in den Figuren dargestellten Ausführungsformen erläutert. Es zeigen:

Fig. 1 eine Chipkarte in Aufsicht,

Fig. 2 einen stark vergrößerten Ausschnitt des Chips der in Fig. 1 dargestellten Chipkarte in Aufsicht,

Fig. 3a, 3b, 3c und 3d
Darstellungen von Look-up-tables.

In Fig. 1 ist als ein Beispiel für den Datenträger eine Chipkarte 1 dargestellt. Die Chipkarte 1 setzt sich aus einem Kartenkörper 2 und einem Chipmodul 3 zusammen, das in eine dafür vorgesehene Aussparung des Kartenkörpers 2 eingelassen ist. Wesentliche Bestandteile des Chipmoduls 3 sind Kontaktflächen 4, über die eine elektrische Verbindung zu einem externen Gerät hergestellt werden kann und ein Chip 5, der mit den Kontaktflächen 4 elektrisch verbunden ist. Alternativ oder zusätzlich zu den Kontaktflächen 4 kann auch eine in Fig. 1 nicht dargestellte Spule oder ein anderes Übertragungmittel zur Herstellung einer Kommunikationsverbindung zwischen dem Chip 5 und einem externen Gerät vorhanden sein.

In Fig. 2 ist ein stark vergrößerter Ausschnitt des Chips 5 aus Fig. 1 in Aufsicht dargestellt. Das besondere der Fig. 2 liegt darin, daß die aktive Oberfläche des Chips 5 dargestellt ist, d.h. sämtliche Schichten, die im allgemeinen die aktive Schicht des Chips 5 schützen, sind in Fig. 2 nicht dargestellt. Um

Informationen über die Signalverläufe im Inneren des Chips zu erhalten, können beispielsweise die freigelegten Strukturen 6 mit Mikrosonden kontaktiert werden. Bei den Mikrosonden handelt es sich um sehr dünne Nadeln, die mittels einer Präzisions-Positioniereinrichtung mit den freigelegten Strukturen 6, beispielsweise Leiterbahnen in elektrischen Kontakt gebracht werden. Die mit den Mikrosonden aufgenommenen Signalverläufe werden mit geeigneten Meß- und Auswerteeinrichtungen weiterverarbeitet mit dem Ziel, Rückschlüsse auf geheime Daten des Chips schließen zu können.

Mit der Erfindung wird erreicht, daß ein Angreifer auch dann, wenn es ihm gelungen sein sollte, die Schutzschicht des Chips 5 ohne Zerstörung des Schaltkreises zu entfernen und die freigelegten Strukturen 6 des Chips 5 mit Mikrosonden zu kontaktieren oder auf andere Weise abzuhören nur sehr schwer oder gar nicht Zugang zu insbesondere geheimen Daten des Chips erlangt. Selbstverständlich greift die Erfindung auch dann, wenn ein Angreifer auf andere Art und Weise Zugang zu den Signalverläufen des Chips 5 erlangt.

Die Figuren 3a, 3b, 3c und 3d zeigen einfache Beispiele für Look-up-tables, bei denen sowohl die Eingangs- als auch die Ausgangsdaten jeweils eine Länge von 2 bit haben. Alle Tabellenwerte sind als binäre Daten dargestellt. In der ersten Zeile sind jeweils die Eingangsdaten x und in der zweiten Zeile die jeweils spaltenweise zugeordneten Ausgangsdaten y dargestellt.

In Figur 3a ist ein Look-up-table für die nicht verfremdete Funktion h dargestellt. Der Figur 3a ist entnehmbar, daß dem Eingangswert x = 00 der Ausgangswert h (x) = 01 zugeordnet ist, dem Eingangswert 01 der Ausgangswert 11, dem Eingangswert 10 der Ausgangswert 10 und dem Eingangswert 11 der Ausgangswert 00. Die Look-up-table gemäß Figur 3a repräsentiert

eine nichtlineare Funktion h, die im Rahmen einer sicherheitsrelevanten Operation ausgeführt werden soll. Im Rahmen der Erfindung wird bei der Durchführung der sicherheitsrelevanten Operation jedoch nicht die in Figur 3a abgebildete Look-up-table selbst verwendet, sondern aus dieser Look-up-table wird gemäß den Figuren 3b, 3c und 3d eine verfremdete Look-up-table abgeleitet.

In Figur 3b ist ein Zwischenschritt der Ermittlung der verfremdeten Look-up-table dargestellt. Die Look-up-table gemäß Figur 3b wurde aus der Look-up-table gemäß Figur 3a erzeugt, indem jeder Wert der ersten Zeile der Tabelle aus Figur 3a mit der Zufallszahl $R_1 = 11$ EXOR verknüpft wurde. So ergib die EXOR-Verknüpfung des Wertes 00 der ersten Zeile und ersten Spalte der Tabelle aus Figur 3a mit der Zahl 11 den Wert 11, der nunmehr das Element der ersten Zeile und ersten Spalte der Tabelle der Figur 3b darstellt. Entsprechend werden die restlichen Werte der ersten Zeile der in Figur 3b dargestellten Tabelle aus den Werten der ersten Zeile der in Figur 3a dargestellten Tabelle und der Zufallszahl $R_1 = 11$ ermittelt. Die in Figur 3b dargestellte Tabelle könnte bereits als verfremdete Look-up-table zur Verarbeitung von ebenfalls mit der Zufallszahl $R_1 = 11$ verfremdeten Geheimdaten eingesetzt werden. Das Ergebnis wäre dann jeweils die in Zeile 2 der Tabelle aus Figur 3b abzulesenden Klartextwerte.

Üblicherweise ordnet man die einzelnen Spalten einer Look-up-table nach aufsteigenden Eingangsdaten x an. Eine durch entsprechende Umsortierung der Tabelle in Figur 3b ermittelte Tabelle ist in Figur 3c dargestellt.

Falls die Tabelle gemäß Figur 3c noch weiter verfremdet werden soll bzw. als Ausgangswerte keine Klartextwerte sondern ebenfalls verfremdete Werte liefern soll, wird eine weitere EXOR-Operation mit einer weiteren Zufallszahl R_2 angewendet.

In Figur 3d ist das Ergebnis der Anwendung dieser weiteren EXOR-Operation dargestellt. Bei dieser Operation werden jeweils die Elemente der zweiten Zeile der Tabelle gemäß Figur 3c mit der Zufallszahl $R_2 = 10$ EXOR verknüpft. Das Element in der zweiten Zeile und der ersten Spalte der Tabelle gemäß Figur 3d entsteht also durch EXOR-Verknüpfung des Elements in der zweiten Zeile und ersten Spalte der Tabelle gemäß Figur 3c der Zufallszahl $R_2 = 10$. Entsprechend werden die weiteren Elemente der zweiten Zeile der Tabelle gemäß Figur 3d gebildet. Die erste Zeile der Tabelle gemäß Figur 3d wird von Figur 3c unverändert übernommen.

Mit der in Figur 3d abgebildeten Tabelle können aus verfremdeten Eingangsdaten ebenfalls verfremdete Ausgangsdaten ermittelt werden. Die so ermittelten verfremdeten Ausgangsdaten können weiteren Operationen zugeführt werden, mit denen verfremdete Daten verarbeitet werden sollen oder es können daraus durch EXOR-Verknüpfung mit der Zufallszahl $R_2 = 10$ Klartextdaten ermittelt werden.

Durch Verwendung der in Figur 3d dargestellten Tabelle ist es möglich, auch nichtlineare Operationen mit verfremdeten Geheimdaten durchzuführen und diese Geheimdaten vor unberechtigtem Zugriff zu schützen. Weiterhin werden auch die sicherheitsrelvanten Operationen selbst vor unberechtigtem Zugriff geschützt, da bei jeder Durchführung der Operationen andersartig

verfremdete Funktionen eingesetzt werden können und man selbst dann, wenn man die verfremdeten Funktionen ermitteln könnte, nicht auf die sicherheitsrelevanten Operationen selbst schließen kann. Nach Umwandlung in Klartext liefern aber sowohl die ursprünglichen sicherheitsrelevanten Operationen als auch die mit Hilfe von verfremdeten Funktionen durchgeführten Operationen identische Ergebnisse. So ergibt beispielsweise ein Eingangswert 00 gemäß der Tabelle in Figur 3a einen Ausgangswert 01. Um zu überprüfen, ob die in Figur 3d dargestellte verfremdete Tabelle den gleichen Ausgangswert liefert, muß der Eingangswert 00 zunächst mit der Zufallszahl R_1 = 11 EXOR verknüpft werden. Als Ergebnis dieser Verknüpfung erhält man den Wert 11. Laut der Tabelle aus Figur 3d ergibt ein Eingangswert 11 einen Ausgangswert von ebenfalls 11. Um aus diesem Ausgangswert den Klartext zu ermitteln, ist der Ausgangswert mit der Zufallszahl R_2 = 10 EXOR zu verknüpfen. Als Ergebnis dieser Verknüpfung erhält man den Wert 01, der mit dem mit Hilfe der in Figur 3a abgebildeten Tabelle ermittelten Werte exakt übereinstimmt.

Die Verfremdung der sicherheitsrelevanten Operationen bzw. der Eingangswerte kann nicht nur durch EXOR-Verknüpfung erzeugt werden, sondern auch durch andere geeignete Verknüpfungsarten, beispielsweise durch eine modulare Addition. Desweiteren ist die Erfindung nicht auf die Anwendung von nichtlinearen Funktionen begrenzt, die mittels der Look-up-tables repräsentiert werden. Es können vielmehr beliebige nichtlineare und auch lineare Funktionen zum Einsatz kommen, für die eine geeignete verfremdete Funktion ermittelbar ist.

M 06.10.99

Patentansprüche

1. Datenträger mit einem Halbleiterchip (5) der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, das in der Lage ist, wenigstens eine Operation (h) auszuführen, wobei für die Ausführung der Operation (h) Eingangsdaten (x) benötigt werden und bei der Ausführung der Operation (h) Ausgangsdaten (y) erzeugt werden, **dadurch gekennzeichnet**, daß

- die Operation (h) vor ihrer Ausführung verfremdet wird,
- die verfremdete Operation (h_{R1}) mit verfremdeten Eingangsdaten ($x \otimes R_1$) ausgeführt wird und
- die Verfremdung der Operation (h) und der Eingangsdaten (x) so aufeinander abgestimmt werden, daß die Ausführung der verfremdeten Operation (h_{R1}) mit verfremdeten Eingangsdaten ($x \otimes R_1$) Ausgangsdaten (y) ergibt, die mit den Ausgangsdaten (y) identisch sind, die bei Ausführung der nicht verfremdeten Operation (h) mit nicht verfremdeten Eingangsdaten (x) ermittelt werden.

2. Datenträger nach Anspruch 1, **dadurch gekennzeichnet**, daß in die Ermittlung der verfremdeten Operation (h_{R1}) und der verfremdeten Eingangsdaten ($x \otimes R_1$) wenigstens eine Zufallszahl (R_1) eingeht.

3. Datenträger nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, daß die Ermittlung der verfremdeten Operation (h_{R1}) und der verfremdeten Eingangsdaten ($x \otimes R_1$) unter Zuhilfenahme von EXOR-Verknüpfungen verfolgt.

4. Datenträger nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß die verfremdete Operation (h_{R1}) vorab im Datenträger fest eingespeichert wird.

5. Datenträger nach Anspruch 4, **dadurch gekennzeichnet,** daß wenigstens zwei verfremdete Operationen (h_{R1}, h_{R1}') vorab in Datenträger fest eingespeichert werden und dann, wenn eine verfremdete Operation ausgeführt werden soll, aus den gespeicherten verfremdeten Operationen (h_{R1}, h_{R1}') eine zufallsbedingt ausgewählt wird.

6. Datenträger nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet,** daß die verfremdete Operation (h_{R1}) vor ihrer Ausführung jeweils neu berechnet wird und für diese Berechnung die wenigstens eine Zufallszahl (R_1) neu ermittelt wird.

7. Datenträger nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet,** daß die Operation (h) durch eine im Datenträger gespeicherte Tabelle realisiert ist, die eine Zuordnung zwischen den Eingangsdaten (x) und den Ausgangsdaten (y) herstellt.

8. Datenträger nach Anspruch 7, **dadurch gekennzeichnet,** daß die Verfremdung der in der Tabelle enthaltenen Eingangsdaten (x) durch Verknüpfung mit der wenigstens einen Zufallszahl (R1) erfolgt.

9. Datenträger mit einem Halbleiterchip (5) der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, das in der Lage ist, wenigstens eine Operation (h) auszuführen, wobei für die Ausführung der Operation (h) Eingangsdaten (x) benötigt werden und bei der Ausführung

der Operation (h) Ausgangsdaten (y) erzeugt werden, **dadurch gekennzeichnet**, daß

- die Operation (h) vor ihrer Ausführung verfremdet wird,
- die verfremdete Operation (h_{R1}) mit verfremdeten Eingangsdaten ($x \otimes R_1$) ausgeführt wird,
- die Verfremdung der Operation (h) und der Eingangsdaten (x) so aufeinander abgestimmt werden, daß die Ausführung der verfremdeten Operation (h_{R1R2}) mit verfremdeten Eingangsdaten ($x \otimes R_1$) Ausgangsdaten ($y \otimes R_2$) ergibt, die gegenüber den Ausgangsdaten (y), die bei Ausführung der nicht verfremdeten Operation (h) mit nicht verfremdeten Eingangsdaten (x) ermittelt werden, verfremdet sind und
- aus den verfremdeten Ausgangsdaten ($y \otimes R_2$) unter Zuhilfenahme vonDaten (R_2), die für die Verfremdung der Operation (h) verwendet wurden, die nicht verfremdeten Ausgangsdaten (y) ermittelbar sind.

10. Datenträger nach Anspruch 9, **dadurch gekennzeichnet**, daß in die Ermittlung der verfremdeten Eingangsdaten ($x \otimes R_1$) wenigstens eine Zufallszahl (R_1) eingeht und daß in die Ermittlung der verfremdeten Operationen (h_{R1R2}) wenigstens zwei Zufallszahlen (R_1, R_2) eingehen.

11. Datenträger nach einem der Ansprüche 9 oder 10, **dadurch gekennzeichnet**, daß die Ermittlung der verfremdeten Operation ($h_{R1, R2}$) und der verfremdeten Eingangsdaten ($x \otimes R_1$) unter Zuhilfenahme von EXOR-Verknüpfungen erfolgt.

12. Datenträger nach einem der Ansprüche 9 bis 11, **dadurch gekennzeichnet**, daß die verfremdete Operation (h_{R1R2}) vorab im Datenträger fest eingespeichert wird.

13. Datenträger nach Anspruch 12, **dadurch gekennzeichnet,** daß wenigstens zwei verfremdete Operationen (h_{R1R2}, $h_{R1'R2'}$) vorab in Datenträger fest eingespeichert werden und dann, wenn eine verfremdete Operation ausgeführt werden soll, aus den gespeicherten verfremdeten Operationen (h_{R1R2}, $h_{R1'R2'}$) eine zufallsbedingt ausgewählt wird.

14. Datenträger nach Anspruch 13, **dadurch gekennzeichnet,** daß die Zufallszahlen (R_1, R_2) mit denen die erste verfremdete Operation (h_{R1R2}) ermittelt wird bezüglich der Verknüpfung, die bei der Ermittlung der verfremdeten Operationen (h_{R1R2} ,$h_{R1'R2'}$) verwendet wird, invers sind zu den Zufallszahlen (R_1', R_2'), mit denen die zweite verfremdete Operation ($h_{R1'R2'}$) ermittelt wird.

15. Datenträger nach einem der Ansprüche 9 bis 11, **dadurch gekennzeichnet,** daß die verfremdete Operation (h_{R1R2}) vor ihrer Ausführung jeweils neu berechnet wird und für diese Berechnung die Zufallszahlen (R_1, R_2) neu ermittelt werden.

16. Datenträger nach einem der Ansprüche 9 bis 15, **dadurch gekennzeichnet,** daß die Operation (h) durch eine im Datenträger gespeicherte Tabelle realisiert ist, die eine Zuordnung zwischen den Eingangsdaten (x) und den Ausgangsaten (y) herstellt.

17. Datenträger nachAnspruch 16, **dadurch gekennzeichnet,** daß die Verfremdung der in der Tabelle enthaltenen Eingangsdaten (x) durch Verknüpfung mit der wenigstens einen Zufallszahl (R1) erfolgt und die Verfremdung der in der Tabelle enthaltenen Ausgangsdaten (y) durchVerknüpfung mit der wenigstens einen weiteren Zufallszahl (R2) erfolgt.

18. Datenträger nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, daß es sich bei der Operation (h) um eine bezüglich der für die Verfremdung der Operation (h) eingesetzten Verknüpfung nichtlineare Operation handelt.

Zusammenfassung

Die Erfindung betrifft einen Datenträger mit einem Halbleiterchip (5), der wenigstens einen Speicher aufweist. In dem Speicher ist ein Betriebsprogramm abgelegt, das in der Lage ist, wenigstens eine Operation (h) durchzuführen. Um einen unberechtigten Zugriff auf die mit der Operation (h) verarbeiteten Daten (x) zu verhindern, werden sowohl diese Daten als auch die Operation (h) selbst verfremdet. Die Verfremdung der Daten (x) und der Operation (h) ist dabei so aufeinander abgestimmt, daß mit der verfremdeten Operation (h_{R1R}, h_{R1R2}) entweder die Ausgangsdaten (y) der nicht verfremdeten Operation (h) erzeugt werden, oder verfremdete Ausgangsdaten ($y \otimes R_2$), aus denen die Ausgangsdaten (y) ermittelbar sind.

M 08.10.99

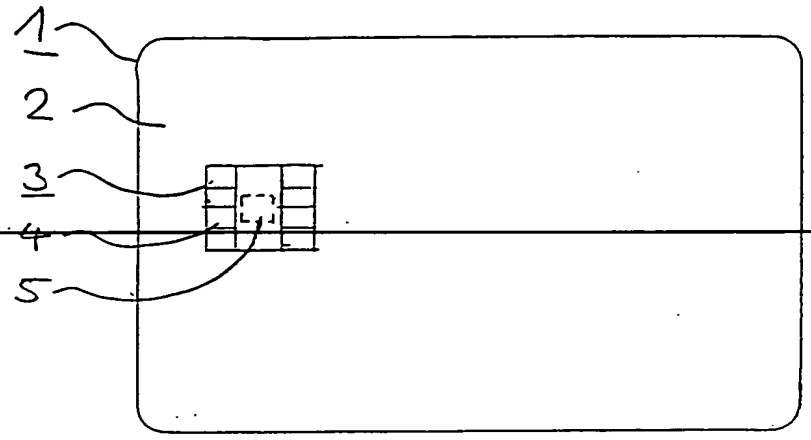

Fig. 1

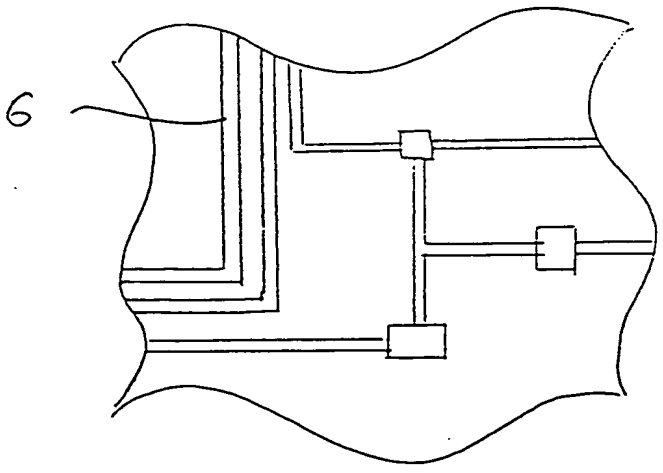

Fig. 2

x	00	01	10	11
h(x)	01	11	10	00

Fig. 3a

x	11	10	01	00
$h_{R1}(x)$	01	11	10	00

Fig. 3b

x	00	01	10	11
$h_{R1}(x)$	00	10	11	01

Fig. 3c

x	00	01	10	11
$h_{R1R2}(x)$	10	00	01	11

Fig. 3d